Stephen R. Sady
Chief Deputy Federal Public Defender
steve_sady@fd.org
Steven T. Wax
Federal Public Defender
steve_wax@fd.org
Lisa Hay
Assistant Federal Public Defender
lisa_hay@fd.org
101 S.W. Main Street, Suite 1700
Portland, Oregon 97204
503-326-2123 Telephone
503-326-5524 Facsimile

Attorneys for Defendant

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,	**Case No. 3:10-cr-00475-KI**
Plaintiff,	**MEMORANDUM IN SUPPORT OF MOTION FOR FULL DISCOVERY REGARDING THE FACTS AND CIRCUMSTANCES UNDERLYING SURVEILLANCE**
v.	
MOHAMED OSMAN MOHAMUD,	
Defendant.	

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Introduction

On November 19, 2013, the government filed a supplemental notice admitting that it introduced at trial and otherwise used the products of surveillance conducted pursuant to the 2008 FISA Amendments Act (FAA). The notice purports to be pursuant to 50 U.S.C.§ 1806(c), but that statute specifically requires that notice be provided "*prior* to trial, hearing, or other proceeding or at a reasonable time *prior* to an effort to so disclose or so use that information or submit it in evidence" (emphasis added). Even though the defense specifically requested pretrial discovery regarding surveillance that led to the Foreign Intelligence Surveillance Act (FISA) warrants, the government did not timely disclose information to the defense or – apparently – to the Court. The notice raises a wide range of serious issues regarding suppression of unlawfully or unconstitutionally obtained evidence, dismissal or other sanctions based on the government's intentional violation of governing rules, and, at least, a new trial based on new evidence of governmental over-reaching. The Court should now order discovery of previously withheld information so a full and open analysis of the government's actions can occur.

As a result of the government's belated notice that it used evidence derived from surveillance under the FAA at trial, at least four areas of legal challenge arise:

> • **Whether the FAA is unconstitutional on its face and as applied.** Before the notice was provided, Mohamed did not know he was an "aggrieved party" with standing to challenge the constitutionality of the FAA, because he did not know that this statute was used to gather information about him. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1154-55 (2013) (plaintiff did not have standing to challenge the FAA's constitutionality, but a person charged in a criminal case who received notice could do so). Mohamed intends to raise constitutional challenges to the statute. Discovery on precisely how the statute has been applied is required in advance of that pleading in order to allow the arguments to be based on facts rather than speculation.

• **Whether the government complied with statutory requirements of the FAA.** Even if constitutional, surveillance under the FAA may have been unlawful – and the fruits subject to suppression – if the government failed to follow the strict procedural requirements of the statute. Discovery is required concerning the specific procedures (*e.g.*, "targeting" and "minimization") in place at the time of the surveillance of Mohamed, the government's compliance with those procedures, and other factual issues, including access to and analysis of the information captured under the FAA. Any assurances of local prosecutors that "all procedures were followed" should not be considered sufficient in this case, given the recent disclosures of National Security Agency (NSA) wrong-doing, including recently declassified Foreign Intelligence Surveillance Court (FISC) opinions and statements from the Executive Branch that some of the procedures in effect during the course of surveillance on Mohamed were either not followed or unconstitutional.

• **Whether the withheld surveillance evidence tainted pretrial motions or defenses at trial, and what consequences should flow from the intentional withholding of such evidence.** The new notice that the government engaged in surveillance of Mohamed under the FAA requires reconsideration of earlier pretrial rulings and decisions. The defense repeatedly argued that the government likely possessed statements by and facts about Mohamed that would be exculpatory or material to pretrial motions and trial issues. Now that public disclosures of government surveillance programs, along with the notice in this case, conclusively establish that the government possessed more information than it produced, all of these pretrial and trial rulings, and the effect of the withheld material on defense decisions, must be revisited. Discovery is necessary first, however, to establish what information the government possessed, how the information was obtained, and how that information was accessed and used.

• **Whether evidence of government over-reaching, misrepresentations, or misconduct was relevant to pretrial or trial issues, and what consequences should flow from the unavailability of that evidence to the defense until after trial.** The government notice discloses several apparently intentional rule violations by the government, including violation of the notice requirements under 50 U.S.C. § 1806(c) and 18 U.S.C. § 3504. The existence of other misrepresentations or over-reaching is strongly supported by the record. Discovery is required into these areas in order to determine the full scope of the conduct and its effect on previous proceedings and the appropriate consequences.

As set out in detail below, broad discovery on these topics in advance of the defense motions to suppress, for a new trial, and for remedial action is essential in order to provide the Court with the full factual context in which these legal issues arise. FISA provides for in camera, ex parte

consideration of materials relevant to these motions if certain national security conditions exist. 50 U.S.C. § 1806(f). The statute also provides, however, that the Court may disclose to the defense these needed discovery materials under appropriate procedures and protective orders if the issues are complex or other factors exist. *Id*. Given that certain of the defense counsel have security clearances, and that the balance of other factors now strongly favors defense involvement in assessing and analyzing these complex issues, the Court should not resort to ex parte proceedings to review and assess the discovery.

A. Because The Government Violated A Mandatory Notice Obligation To The Court And To The Defense, The Starting Point For This Court's Discovery Order Should Be Full Disclosure Of The Circumstances Behind The Violation Of The Requirement Of Pretrial Notice Under 50 U.S.C. § 1806(c).

The government violated the statutory requirement that pretrial notice be provided of FAA surveillance to both the Court and the defense. The Court should conclude that, based on the apparent provenance of the government's belated disclosure, the government's failure to comply with the FAA notice requirement resulted from knowing and intentional conduct by government actors. The deliberate violation of the notice statute, which also implicates *Brady* and due process, requires discovery for litigation regarding the remedy for the statutory violation, the grounds for suppression of derivative, and potentially other, uses of FAA surveillance, and the disclosure of potential evidence of governmental over-reaching that may be introduced at a new trial.

1. The Mandatory Language Of § 1806(c) Required That The Government Provide The Notice Of The Use Of Material Derived From FAA Surveillance Prior To Trial.

The notice statute is mandatory in requiring that notice be provided to "the aggrieved person and the court" prior to trial where evidence derived from FAA surveillance is used in any way:

> **(c) Notification by United States**
>
> *Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court*, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, *any information obtained or derived from an electronic surveillance of that aggrieved person* pursuant to the authority of this subchapter, *the Government shall, prior to the trial, hearing, or other proceeding* or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, *notify the aggrieved person and the court* or other authority in which the information is to be disclosed or used *that the Government intends to so disclose or so use such information.*

50 U.S.C. § 1806(c) (emphasis added). The defendant in this case is an "aggrieved person" within the plain meaning of the statute. 50 U.S.C. § 1801(k) ("'Aggrieved person' means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."). The "electronic surveillance" under "this subchapter" refers to subchapter I of the FISA, which is entitled "Electronic Surveillance" and codified between 50 U.S.C. §§ 1801 and 1812. The statute broadly defines electronic surveillance in 50 U.S.C. § 1801(f).

The FAA explicitly incorporates the § 1806(c) mandatory notice requirement to cover surveillance activity under Title VII, which is codified at 50 U.S.C. §§ 1881a to 1881g. The cross-reference on notice is explicit and mandatory: "Information acquired from an acquisition conducted under section 1881a of this title shall be deemed to be information acquired from an electronic surveillance pursuant to subchapter I of this chapter for purposes of section 1806 of this title." 50

U.S.C. § 1881e(a). Congress's use of "shall" leaves no room for the government to fail to give notice: "The word 'shall' is ordinarily 'the language of command.'" *Alabama v. Bozeman*, 533 U.S. 146, 153 (2001) (quoting *Anderson v. Yungkau*, 329 U.S. 482, 485 (1947)).

Despite the mandatory notice statute, the initial notice in this case provided no reference to FAA surveillance: "pursuant to Title 50, United States Code, Sections 1806(c) and 1825(d), the United States intends to offer into evidence, or otherwise use or disclose in any proceedings in the above-captioned matter, information obtained and derived from electronic surveillance and physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 ('FISA'), as amended, 50 U.S.C. §§ 1801-1812 and 1821-1829." CR 4. The new notice explicitly concedes that the products of FAA surveillance – 50 U.S.C. § 1881a – were introduced at trial and otherwise used:

> This supplemental notice is being filed as a result of the government's determination that information obtained or derived from Title I FISA collection may, in particular cases, also be "derived from" prior Title VII FISA collection. Based upon that determination and a recent review of the proceedings in this case, the United States hereby provides notice to this Court and the defense, pursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), that the government has offered into evidence or otherwise used or disclosed in proceedings, including at trial, in the above-captioned matter information derived from acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a.

CR 486.

Where evidence is "derived" from surveillance that was "not lawfully authorized or conducted," the Court must suppress the evidence. 50 U.S.C. § 1806(g). Derivative evidence includes statements and tangible evidence that are the "fruit of the poisonous tree." *Murray v. United States*, 487 U.S. 533, 536-37 (1988) ("the exclusionary rule also prohibits the introduction of derivative evidence, both tangible and testimonial, that is the product of the primary evidence, or

that is otherwise acquired as an indirect result of the unlawful search, up to the point at which the connection with the unlawful search becomes 'so attenuated as to dissipate the taint'") (quoting *Nardone v. United States*, 308 U.S. 338, 341 (1939)) (citing *Wong Sun v. United States*, 371 U.S. 471, 484-85 (1963)). The Supreme Court found in *Murray* that law enforcement decisions could be derived from – or fruits of – the primary illegality, where "the agents' decision to seek the warrant was prompted by what they had seen during the initial entry," 487 U.S. at 542, or, here, for example, if the decision not to intervene and coopt Mohamed before the sting began, or the decision to engage in a sting operation, was prompted by the results of illegal surveillance.

2. The Representations To The Supreme Court That Led To The Late Notice Establish That The Government's Suppression Of Discoverable Information Was Knowing And Intentional.

Based on public information that preceded the supplemental notice in this case, government actors made a conscious decision to conceal the fact that evidence presented at trial was derived from FAA surveillance. The Solicitor General, in response to finding out that he had misrepresented to the Supreme Court the government's notice practice, put into motion the events leading to the revelation that national security lawyers and other government operatives routinely and deliberately failed to provide notice of FAA surveillance to criminal defendants. This revelation appears to have led directly to the post-trial notice in this case.

On the day the FAA was enacted in 2008, the American Civil Liberties Union (ACLU) filed suit on behalf of individuals who believed they were subjected to FAA surveillance. They challenged the statute's broadening of electronic surveillance authority under FAA to eliminate much of the specificity and other protections traditionally required by the Fourth Amendment:

- excision of the requirement that the government describe to the FISC each specific target and identify each facility at which its surveillance would be directed, thus permitting surveillance on a programmatic, rather than individualized, basis (18 U.S.C. § 1881a(g));

- removal of the requirement that a target be a "foreign power or an agent of a foreign power" (*id.*); and

- diminution of the FISA court's authority to insist upon, and elimination of its authority to supervise, instance-specific privacy-intrusion minimization procedures (though the government still must use court-approved general minimization procedures) (18 U.S.C. § 1881a(e)).

Before reaching these constitutional questions, the initial FAA litigation focused on the question of standing: could the plaintiffs establish that they were subjected to secret surveillance when the government refused to disclose whether they were being watched? After the Second Circuit found the plaintiffs had standing, the Supreme Court granted certiorari.

In the Supreme Court briefing, Solicitor General Donald Verrilli argued that, contrary to the ACLU's argument that no one could prove standing because the surveillance was secret, criminal defendants received notice of FAA surveillance and would therefore have standing to challenge the surveillance program:

> If the government intends to use or disclose any information obtained or derived from its acquisition of a person's communications under Section 1881a in judicial or administrative proceedings against that person, *it must provide advance notice of its intent to the tribunal and the person, whether or not the person was targeted for surveillance* under Section 1881a. 50 U.S.C. 1881e(a); see 50 U.S.C. 1801(k), 1806(c). *That person may then challenge the use of that information in district court* by challenging the lawfulness of the Section 1881a acquisition. 50 U.S.C. 1806(e) and (f), 1881e(a).

Brief for Petitioners at 8, *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013) (No. 11-1025) (emphasis added). During the oral argument in *Clapper* on October 29, 2012, the government

continued to represent that it provided notice to criminal defendants as required by statute. Transcript of Oral Argument at 4-5, *Clapper*, 133 S. Ct. 1138 (2013) (No. 11-1025).

On February 26, 2013, the Supreme Court reversed the Second Circuit's finding of standing by a five to four vote. Writing for the majority, Justice Alito relied on the provision of notice "if the Government intends to use or disclose information obtained or derived from a § 1881a acquisition in judicial or administrative proceedings." *Clapper*, 133 S. Ct. at 1154. The Court rejected the argument that the FAA would be insulated from constitutional challenge because, if an individual who had been surveilled were prosecuted, "the Government would be required to make a disclosure." *Id*.

After the Supreme Court ruled, it became apparent that the Solicitor General's representations to the Court were wrong: prosecutors routinely and deliberately failed to provide notice in cases where the derivatives of FAA surveillance were to be used at trial or other proceedings. The exposure of the government's secret policy that kept the defense and the courts in the dark apparently stemmed from the statement by Senator Dianne Feinstein, the Chair of the Senate's intelligence oversight committee, on December 27, 2012, that the FAA had been used to thwart terrorist attacks in Chicago and Ft. Lauderdale in claiming. 158 Cong. Rec. S8393 (daily ed. Dec. 27, 2012). Subsequent inquiry determined that the lawyers in the named cases had received no notice regarding FAA-derived evidence, establishing that either Senator Feinstein was mistaken or the Solicitor General had misinformed the Supreme Court. Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. Times, July 15, 2013.[1]

[1] Senator Feinstein later asserted her statements were not intended to convey FAA involvement in those cases. Motion for Discovery in Support of Defendant's Previously Filed

Solicitor General Verrilli reportedly made his representations about notice because national security lawyers had reviewed and approved the Solicitor General's brief prior to filing. Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013. The Solicitor General later discovered that, with no legal basis, the notice requirement had been construed in such a restrictive manner that no notice was ever provided: "The move [to begin disclosing FAA surveillance] comes after an internal Justice Department debate in which Solicitor General Donald B. Verrilli Jr. argued that there was no legal basis for a previous practice of not disclosing links to such surveillance, several Obama administration officials familiar with the deliberations said." *Id*. The Solicitor General apparently determined there was not "any persuasive legal basis for failing to clearly notify defendants that they faced evidence linked to the 2008 warrantless surveillance law." *Id*.

On October 25, 2013, the government for the first time disclosed the intention to use evidence derived from FAA electronic surveillance in the prosecution of Jamshid Muhtorov in Colorado. Devlin Barrett, *U.S. Tells Suspect for First Time It Used NSA Surveillance Program in Criminal Case*, Wall St. J., Oct. 25, 2013. Shortly thereafter, Attorney General Eric Holder stated that the Department of Justice was reviewing cases to determine whether they should be "providing defendants with information that they should have" in order for them to decide what steps to take. Sari Horwitz, *Justice is reviewing criminal cases that used surveillance evidence gathered under FISA*, Wash. Post, Nov. 15, 2013. Several days later, the government filed the notice in the present

---

Motion for Notice of FISA Amendments Act Evidence at Exhibit B, *United States v. Daoud*, No. 12-cr-00723 (Sept. 18, 2013), ECF No. 70-2 at 3-4 (letter from Office of Senate Legal Counsel).

case, which according to reports resulted from a review of deliberate decisions by national security prosecutors to withhold the information:

> But it has since emerged that it was not the practice of National Security Division prosecutors to tell defendants when warrantless wiretapping had led to evidence in a case, something Mr. Verrilli had not known at the time of the Supreme Court case, even though his briefs and arguments assuring the justices otherwise had been vetted by the division. After the discrepancy came to light, Mr. Verrilli fought an internal battle to bring department policy in line with what he had told the court, ultimately prevailing.

Charlie Savage, *Warrantless Surveillance Continues to Cause Fallout*, N.Y. Times, Nov. 20, 2013. Thus, the public record strongly demonstrates that the failure to provide the statutorily required pretrial notice in the present case resulted from a secret and deliberate policy that led to the routine practice of violating the statute.

3. The Full Circumstances Behind The Government's Violation Of The Notice Statute Are Relevant To Forthcoming Defense Motions Regarding Remedy, Suppression, and New Trial.

The contrast between the initial FISA notice and the post-trial FAA notice, in the context of the reporting on the government's change in notice practices, demonstrates that an intentional violation of the FISA notice statute occurred in this case. This Court should order complete discovery regarding the full circumstances surrounding the withholding of the FAA notice because such information is necessary to calibrate the remedy for the statutory violation, to provide the bases for suppression of evidence, and to disclose any *Brady* material that should be available for a new trial as evidence of governmental over-reaching in support of the entrapment defense. While the statutory violation provides the Court with remedial authority, the government's deliberate suppression of notice also violates due process because the notice requirement codified by § 1806(c) embodies the constitutional requirement of notice, given the *Brady* obligation, Rule 16, and the

balance of procedural due process interests at stake. *See Mathews v. Eldridge*, 424 U.S. 319, 333 (1976); *Goldberg v. Kelly*, 397 U.S. 254, 267-68 (1970).[2]

Although press reports provide the background, the Court needs primary source information regarding the policies and practices that led to the violation of the notice requirement in this case. The Court should find that, if the notice violation was intentional, the case must be dismissed because Congress enacted the notice statute in the context of Supreme Court decisions that required the government to choose in national security cases between disclosure and dismissal.[3] To the extent dismissal is not mandatory, the Court should require discovery in support of the remedial factors identified by the Ninth Circuit. Under its inherent supervisory powers, this Court has the authority to fashion consequences up to and including dismissal: "(1) to implement a remedy for the violation of a recognized statutory or constitutional right; (2) to preserve judicial integrity by ensuring that a conviction rests on appropriate considerations validly before a jury; and (3) to deter future illegal

---

[2] Under 50 U.S.C. §1881e, the government is required to give notice of use of §§ 1881a and 1881b. Section 1881e does not require notice if the government has utilized § 1881c. For all of the reasons discussed in this pleading, a defendant in a criminal case is entitled to notice of the intended use of information derived from surveillance conducted pursuant to § 1881c. The defense motion for discovery includes discovery of all material derived from all surveillance including §§ 1881a, b and c.

[3] *See Alderman v.United States*, 394 U.S.165, 184 (1969) (dismiss or disclose surveillance reports); *Jencks v.United States*, 353 U.S.657, 672 (1957) (dismiss or disclose witness statements); *Roviaro v. United States*, 353 U.S. 53, 61 & 65 n.15 (1957) (dismiss or disclose informant); *see United States v. Coplon*, 185 F.2d 629, 638 (2d Cir. 1950) (Hand, J.) ("the prosecution must decide whether the public prejudice of allowing the crime to go unpunished was greater than the disclosure of such 'state secrets' as might be relevant to the defence.").

conduct." *United States v. Matta-Ballesteros*, 71 F.3d 754, 763 (9th Cir. 1995) (citing *United States v. Simpson*, 927 F.2d 1088, 1090 (9th Cir.1991)).[4] Each of these factors is implicated by this case.

- **Full discovery is needed to formulate a remedy for the violation of the notice requirement**.

Where there is a right to pretrial notice, there must be a remedy for the violation of that right. For the defense to effectively advocate for a certain remedy, and for the Court to make an informed exercise of its authority, the facts should be fully developed. *United States v. Hernandez-Meza*, 720 F.3d 760, 768-69 (9th Cir. 2013). Facts favorable or helpful to the defense in the context of suppression motions constitute *Brady* material that must be produced pretrial. *United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000); *United States v. Barton*, 995 F.2d 931, 934-35 (9th Cir. 1993) (rationale of *Brady* applies to suppression motions). In developing the facts, the Court should order complete and unrestricted access to the materials that reflect the formulation and implementation of the policies and practices that led to the statutory and constitutional violation. The questions of who knew what when, as well as the level of knowledge and intention, should be fully explored by the Court with the assistance of the defense.

In *Hernandez-Meza*, the Ninth Circuit vacated a conviction because the government failed to disclose an immigration document used in an illegal reentry prosecution. The court emphasized that the Rule 16(a)(1)(E)(i) obligation to provide documents or things that "are material to preparing the defense" is categorical and unconditional including even material that would discourage the

[4] The Court's inherent powers are not limited to these three areas. *United States v. W.R. Grace*, 526 F.3d 499, 511 n.9 (9th Cir. 2008) (en banc).

presentation of a certain line of defense. *Hernandez-Meza*, 720 F.3d at 768. "Lack of knowledge or even a showing of due diligence won't excuse non-compliance." *Id*.

Most importantly for discovery purposes, the court remanded for a determination of whether the government's action was deliberate. Because the record suggested "that the government may have deliberately withheld" the naturalization document from the defendant, the court remanded the case for the district court to determine if the government acted willfully, which should warrant preclusion of evidence from retrial and perhaps dismissal of the indictment:

> We infer this from the record as a whole and particularly from the fact that the prosecution knew the date of Hernandez–Meza's mother's naturalization and its relevance to the case, yet didn't produce the certificate even after defense counsel pointed out the lacuna. However, this is a factual finding that must be made by a district court in the first instance. *If the government willfully withheld the certificate, then it should be precluded from introducing the document at any retrial of Hernandez–Meza, or perhaps even suffer a dismissal of the indictment with prejudice. See Kojayan*, 8 F.3d at 1325 (remanding for a decision as to whether indictment should be dismissed with or without prejudice).

Hernandez-Meza, 720 F.3d at 769 (emphasis added) (internal citation omitted). Under the holding and reasoning of *Hernandez-Meza*, this Court should allow full discovery and open litigation regarding all documents underlying the government's withholding of the required notice and the content of the material that is the subject of the supplemental notice.

The Court should not accept selective or summary accounts of the underlying facts: the primary sources and the inferences to be drawn from them should be subject to full adversary proceedings, whether or not the proceedings are sealed. To the extent the government would seek to claim such information is privileged, the Court should reject such contentions. First, the public interest is very much served by disclosure of executive efforts to thwart congressional requirements of notice. Second, the material can hardly be treated as confidential when, according to the media,

"several Obama administration officials familiar with the deliberations" have already made selective disclosures to the press on the subject of the institutional failure to comply with notice requirements. Third, the policies of privilege generally do apply to prevent exposure of law violations. Lastly, because once the decision is made to prosecute the government "has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense." *United States v. Reynolds*, 345 U.S. 1, 12 (1953).

- **The Court needs to determine the extent to which the products of unlawful activity were improperly before the jury.**

Discovery regarding materials reflecting the hiding of surveillance and its eventual exposure will help to determine the extent to which the derivatives of unlawful activity were before the jury. This is a three-step analysis. First, the government, by giving notice only after trial, admits that derivative evidence was not validly before the jury because, although derivative evidence was introduced, the government failed to give the required § 1806(c) notice. So evidence regarding the notice violation alone provides information relevant to the exercise of this Court's supervisory power as well as to whether discovery violations occurred that should be addressed under Rule 16(d)(C) and (D). Second, the lawfulness of the underlying surveillance activity may be informed by information regarding efforts to keep it clandestine. Given the massive tools available in national security cases, the government's efforts to keep this surveillance secret from the Court as well as the defense may reflect on the legality of the derivative evidence presented to the jury. Third, the facts that underlie the notice violation may provide or lead to evidence that is relevant at retrial regarding the government's over-reaching and unreliability.

- **The Court needs the factual bases to deter unlawful conduct.**

The Chief Judge of the Ninth Circuit recently observed that the government's withholding of evidence – as here, notice of FAA surveillance – virtually never has meaningful consequences: "In the rare event that the suppressed evidence does surface, the consequences usually leave the prosecution no worse than had it complied with *Brady* from the outset." *United States v. Olsen*, 737 F.3d 625, 630 (9th Cir. 2013) (Kozinski, C.J., dissenting from denial of rehearing en banc). As a result, "[t]here is an epidemic of *Brady* violations abroad in the land. Only judges can put a stop to it." *Id*. at 626. This Court should not accept assurances from the government without first obtaining the complete factual underpinnings of the notice violation. This is especially important, where the government may have provided materially incomplete or incorrect information to the Court. *See Islamic Shura Council of S. Cal. v. FBI*, 779 F. Supp. 2d 1114, 1117 (C.D. Cal. 2011) (the government "provided false and misleading information" to the court regarding the existence of documents, then asserted the "untenable" position that misleading the court was permissible "to avoid compromising national security"). The Court's exercise of supervisory power includes a strong interest in deterring the withholding of information that should have been disclosed. In order to determine how to exercise its authority, the Court should order complete discovery not only to protect the interests of the accused, but to preserve "the public's trust in our justice system" and prevent erosion of "the foundational premises of the rule of law." *Olsen*, 737 F.3d at 632.

B. Because The Belated Notice Is Part Of A Cascade Of Disclosures Relevant To This Case, The Court's Discovery Order Should Require Disclosure Of All Surveillance Activities Including But Not Limited To FAA Electronic Surveillance Under 50 U.S.C. § 1881a, Collection Of Internet And Telephone Metadata And Any Subsequent Accessing Of That Material, And Application Of Other Surveillance Programs Revealed Since The Trial Of This Case.

The government's late notice in this case and the relevant disclosures about governmental practices stemming from the *Clapper* situation arose at the same time as disclosures about the extent of government surveillance by former NSA contractor Edward Snowden. The Snowden disclosures provide additional support for the discovery that should be ordered regarding surveillance programs not previously disclosed to the defense and the products of those programs.

1. The Details Of The FAA Electronic Surveillance Should Be Produced Because Motions Based On The FAA's Unconstitutionality And The Scope Of Authorized Surveillance Require Full Factual Development.

The government's notice that it used the products of § 1881a surveillance at trial and in other ways is only the starting point for consideration of the appropriate remedy that can only be determined after it is fully understood how extensive the government's surveillance was and its timing. There is no question that the defense will challenge the constitutionality of the FAA as part of the substantive motions following completion of discovery: the Court should find that the statute's lack of judicial warrants, specificity of individuals and locations, and judicial supervision render it constitutionally invalid.

The present case involves the types of communications involving a statutory "United States person" – American citizen Mohamed – that have been subject to electronic surveillance:

- Foreign with foreign communication where one party is a United States citizen (*e.g.*, Mohamed's email as a juvenile from London to others, some of whom were also overseas);

- Foreign with domestic communication where one party is a United States citizen (*e.g.*, Mohamed's email from Beaverton, Oregon, with Amro al-Ali overseas);

- Domestic with domestic communication where at least one party is a United States citizen (*e.g.*, Mohamed's email from Beaverton, Oregon, with United States citizen Samir Khan in North Carolina).

The FBI appeared to have information on Mohamed prior to obtaining a FISA warrant specifically directed at him or opening a formal investigation on him. What the government had and how it was obtained must be disclosed in order for any meaningful analysis to occur. Full discovery regarding the targeting, scope, manner, authorizations, limitations, and mitigation of the intrusions (or lack thereof) are needed to effectively formulate the arguments regarding the legality and derivative use of the surveillance under the statute. The defense should have full access to the relevant facts to inform the legal arguments regarding the FAA's constitutionality.

The discovery order should include all targeting and minimization procedures, including interpretive instructions, that were in effect at all times the government conducted surveillance of Mohamed. The Snowden disclosures include purported FAA targeting and minimization procedures under FISA and the FAA – 50 U.S.C. §§ 1801(h)(1) and 1881a (d) & (e). Glenn Greenwald & James Ball, *The top secret rules that allow NSA to use US data without a warrant*, The Guardian, June 20, 2013. Since the initial revelations, some of the disclosed rules have been declassified, others remain classified, and still others are likely classified but not publicly disclosed. *See* Press Release, DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA) (Aug. 21, 2013). This Court's order should require specification of which procedures were in effect on all dates that Mohamed was subject to surveillance because the Director of National Intelligence (DNI) has acknowledged that rules during

that rough time frame violated the Fourth Amendment. In a letter from the Director's office to Senator Wyden, the DNI included the admissions that

- "on at least one occasion the Foreign Intelligence Surveillance Court held that some collection carried out pursuant to the Section 702 minimization procedures used by the government was unreasonable under the Fourth Amendment," and
- the agency believed "the government's implementation of Section 702 of FISA has sometimes circumvented the spirit of the law, and on at least one occasion the FISA Court has reached this same conclusion."

Letter from the Office of the DNI to Senator Ron Wyden, July 20, 2012.[5] *See also* Charlie Savage, *N.S.A. Said to Search Content of Messages To and From U.S.*, N.Y. Times, Aug. 8, 2013.

The Court's order should include not only the complete targeting and minimization procedures in effect at the relevant times, but also any interpretive directives, memoranda, letters, transcripts of instructions, and other writings that guided the implementation of the procedures. For example, the initial Snowden disclosure included a "transcript of a 2008 briefing on FAA from the NSA's general counsel" that "sets out how much discretion NSA analysts possess when it comes to the specifics of targeting, and making decisions on who they believe is a non-US person." Glenn Greenwald & James Ball, *The top secret rules that allow NSA to use US data without a warrant*, The Guardian, June 20, 2013. Further, because recent declassified FISC decisions have found that historical government conduct from the outset of the FAA was unlawful, the Court should order that the defense have access to all decisions, classified or not, that find problems with the conduct of surveillance under the procedures in effect from 2007 to 2010.

---

[5] Available at http://www.wired.com/images_blogs/dangerroom/2012/07/2012-07-20-OLA-Ltr-to-Senator-Wyden-ref-Declassification-Request.pdf.

Aside from facial and as-applied challenges to the statute, full factual development and access to the relevant protocols will enable the defense to present arguments regarding the second half of the statutory suppression standard: whether the government acted within the scope of the authorizations and orders. Even assuming the FAA is valid, suppression is warranted if the "surveillance was not made in conformity with an order of authorization or approval." 50 U.S.C. § 1806(e)(2) & (g). Recently declassified FISC opinions reveal that the relevant agencies have a long and persistent history of violating the limitations in court orders. For example:

- the "NSA exceeded the scope of authorized acquisition continuously during the more than [redacted] years of acquisition" (*[Case Name Redacted]*, PR/TT No. [docket redacted], at 3, (FISC [date redacted]) (declassified Nov. 18, 2013));

- "the NSA has on a daily basis, accessed the BR [business records] metadata for purposes of comparing thousands of non-RAS [reasonable articulable suspicion] approved telephone identifiers on its alert list against the BR metadata in order to identify any matches," which was a violation of the earlier court order that was compounded by the government's repeated inaccurate descriptions to the FISC (*In re Production of Tangible Things from [redacted]*, No. BR 08-13, 2009 WL 9150913, at *2-8 (FISC Mar. 2, 2009) (declassified Sept. 10, 2013));

- "NSA's placement of unminimized metadata [redacted] into databases accessible by outside agencies, which, as the government has acknowledged, violates not only the Court's orders, but also NSA's minimization and dissemination procedures set forth in [United States Signal Intelligence Directive] 18" (*In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted]*, No. BR 09-06, at 6-7 (FISC June 22, 2009) (order requiring government to report and explain instances of unauthorized sharing of metadata) (declassified Sep. 10, 2013));

- the court was "deeply troubled" by previous compliance incidents that occurred shortly after the completion of NSA's "end to end review" of the processes for handling BR metadata "and its submission of a report intended to assure the court that NSA had addressed and corrected the issues giving rise to the history of serious and widespread compliance problems" (*In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted]*, No. BR 09-13, 2009 WL 9150896, at *2 (FISC Sept. 25, 2009) (declassified on Sep. 10, 2013)).

Without full discovery regarding all the surrounding factual and legal circumstances of the surveillance, the defense cannot effectively present to the Court the arguments for suppression based on lack of compliance with authorizations. Further, even if the motion were to be denied, the full discovery would be necessary for the defense and the Court to have the opportunity to review the products of the surveillance to determine the existence of material useful to the defense at trial. 50 U.S.C. § 1806(g) ("If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person *except to the extent that due process requires discovery or disclosure*.") (emphasis added).

2. The Court Should Order The Production Of All Material Relating To The Government's Seizure And Accessing Of Internet And Telephone Metadata.

Six months ago, the world learned the NSA was collecting massive amounts of Americans' telephone information and Internet activity from former NSA contract employee Snowden. Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian, June 5, 2013; Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, June 6, 2013. Since that time, the government has acknowledged the program, and the legal debate regarding its lawfulness has begun. Part of the debate rests on the reality that, just as Global Positioning Systems can provide intimate details of an individual's life, the same can occur with phone and Internet metadata. *Compare United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.") *with Klayman v. Obama*, No. 13-0851, 2013 WL 6571596 (D.D.C. Dec. 16, 2013) (in the context of telephone metadata,

"[r]ecords that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic – a vibrant and constantly updating picture of the person's life."). Based on the mass collection of metadata, the government apparently maps the social connections of American citizens. James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. Times, Sept. 28, 2013.

The scope and complexity of the government's metadata surveillance programs require discovery to unravel the role they played in the investigation and prosecution of Mohamed, the way these programs operate in practice, and their purported statutory bases. For instance, for at least seven years, the NSA has collected the phone records of virtually every call made or received within the United States, relying on authority purportedly conferred in 50 U.S.C. § 1861. *Klayman v. Obama*, No. 13-0851, 2013 WL 6571596, *3-4 (D.D.C. Dec. 16, 2013). The government's collection of Internet metadata appears to be even more intrusive than traditional telephone metadata. *See* James Ball, *NSA stores metadata of millions of web users for up to a year, secret files show*, The Guardian, Sept. 30, 2013 ("Metadata provides a record of almost anything a user does online, from browsing history – such as map searches and websites visited – to account details, email activity, and even some account passwords."). These widespread intrusions on digital privacy have been conducted, at least in part, under the anemic procedural provisions for pen registers and trap-and-trace devices in 50 U.S.C. § 1842.

The metadata programs directly affect this case in at least three ways that require notice and discovery as a matter of procedural due process and under *Brady*. First, the surveillance almost certainly involved the seizure of Mohamed's telephone information and Internet activity during the relevant time. Mohamed had accounts with the relevant service providers and, in any event, the

NSA was collecting and searching data as it traveled across cables linking service providers and/or their data storage centers. Ewen MacAskill, et al., *GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian, June 21, 2013. The patterns revealed by the telephone and computer records are potential *Brady* material because the defense can use it to corroborate facts favorable to the theory of defense. The Court should order the government to disclose the bulk metadata relating to the telephone and Internet communications of the defendant, especially where the defense's limited access to communications records established gaps in the government's production of records before trial.

Second, if telephone records were collected as "tangible things" under 50 U.S.C. § 1861(a), or if Internet metadata was collected pursuant to 50 U.S.C. § 1842, discovery is needed to establish whether the taking of material regarding Mohamed violated the statutory targeting protocols or constitutional protections. At the time of the seizure, the government would have had to show "that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) . . . ." 50 U.S.C. § 1861(b)(2)(A). This is important because the government repeatedly asserted that, until well after the first face-to-face meeting, the agents were engaged in "threat assessment" regarding Mohamed. *See*, *e.g.*, CR 440 at 505, 567; CR 443 at 804, 813; CR 444 at 899. To the extent metadata was accessed outside of § 1861, the targeting procedures or the lack thereof should be subject to disclosure. Discovery is needed to determine whether the telephone and Internet information was lawfully authorized and whether the surveillance lawfully conducted. Only with full discovery can violation of the targeting provisions be effectively brought to the Court's attention.

Third, given some of the numbers called and Internet sites visited, the government may well have accessed the metadata as it pertains to the defendant's social connections. FISA includes significant restrictions on accessing the contents of records pertaining to American citizens in the statute's minimization procedures. 50 U.S.C. § 1861(g). Because Mohamed is an "unconsenting United States person[]" (and was likely a minor during much of the surveillance), the discovery must include the minimization and dissemination procedures for Americans adopted pursuant to § 1861(g) as well as whether and how those procedures applied to the collection and use of Mohamed's telephone and Internet metadata. The discovery in this area is especially important given the recent declassification of opinions in which the FISC criticized the intelligence agencies' failure to follow statutory requirements and to adhere to limitations in court authorizations. The Court should order full disclosure of all the material related to any accessing and use of Mohamed's telephone and Internet metadata and content.

3. The Court Should Order The Government to Produce Material Relevant To Application Of Secret Surveillance Programs To This Case.

The Snowden disclosures have established that the types, times, and intrusiveness of the surveillance are much greater than would otherwise have been known. As the new disclosures mount, a number of them correlate closely to situations in this case. The Court's discovery order should include all material pertaining to secret surveillance programs to the extent they applied to Mohamed.

Installation Of Malware And Remote Activation Of Laptop Cameras: Last month, based on warrant application material filed by a Texas judge, the FBI's ability to secretly activate a target's laptop camera "without triggering the light that lets users know it is recording" has become public

knowledge. Craig Timberg & Ellen Nakashima, *FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance*, Wash. Post, Dec. 6, 2013; *see also* Jennifer Valentino-DeVries & Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, Wall St. J., Aug 3, 2013. The defense provided the Court with substantial indications that the FBI accessed Mohamed's personal laptop computer under circumstances indicating that malware had been installed, such as CIPAV (computer and internet protocol address verifier). CR 142 at 2-3; *see* Richard Lyon, *Is FBI Contractor Planting Malware?* Daily Kos, Aug. 5, 2013.[6] In sealed pleadings, the defense presented compelling evidence that the FBI had visually spied on Mohamed while he was in the privacy of his home. Supplement to Suppression and Discovery Motions at 4-5. Given that these programs have been widely exposed, the balance of interests strongly favor disclosure to the defense in order for the Court to receive advocacy regarding the lawfulness and authority for such intrusions, which the Ninth Circuit has held are among the most extreme forms of privacy violations. *See United States v. Nerber*, 222 F.3d 597, 603 (9th Cir. 2000) ("Hidden video surveillance is one of the most intrusive investigative mechanisms available to law enforcement.").

Surveillance Of Conversations By Individuals Playing Video Games: The Snowden disclosures have also exposed the practice of sending agents to record conversations within video games played by Americans and others online. Mark Mazzetti & Justin Elliott, *Spies Infiltrate a Fantasy Realm of Online Games*, N.Y. Times, Dec. 9, 2013. As reflected in the discovery and testimony, Mohamed played a number of video games such as Halo that have the capacity for conversations among groups of players. Any online statements by Mohamed that were surveilled

[6] Available at http://www.dailykos.com/story/2013/08/05/1229082/-Is-FBI-Contractor-Planting-Malware#.

by the government are required discovery as statements of the accused under Rule 16(a)(1)(B). Only by obtaining the primary source statements can the Court, with appropriate input from the defense, determine whether the material was lawfully accessed and used and, further, whether any statements disclosed are useful to the defense.

Surveillance To Determine Use Of Pornography: The Snowden disclosures revealed that the government surveilled the accessing of online pornography sites to compromise certain persons of interest. Glenn Greenwald, et al., *Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers,'* Huffington Post, Dec. 2, 2013. Given his writings for Jihad Recollections while he was a minor, Mohamed may have been labeled as a radicalizer. The government should be required to disclose whether Mohamed's computer use was surveilled to obtain potentially embarrassing information about the use of pornography. The material would assist in determining the legality of that type of accessing and use of surveillance authority and in establishing the existence of potential *Brady* evidence regarding governmental over-reaching.

C. The Government's Violation Of The Obligation To "Confirm Or Deny" Surveillance Activity Under 18 U.S.C. § 3504 Exacerbates The Government's Failure To Disclose In This Case.

The defense has repeatedly cited *Alderman v. United States*, for the proposition that counsel should have the opportunity to review classified material because of the importance of the defense perspective in determining the significance of surveillance activity. 394 U.S. 165 (1969). Ironically, the procedural posture of *Alderman* is remarkably similar to what has now occurred in this case. In the consolidated cases in *Alderman*, both defendants were on appeal when they discovered that the government had wiretapped them. The Court had to determine what procedure should occur on the remand and, after discussing the importance of the Fourth Amendment and the requirement of

standing, the Court remanded with the strong language about defense participation: "As the need for adversary inquiry is increased by the complexity of the issues presented for adjudication, and by the consequent inadequacy of ex parte procedures as a means for their accurate resolution, the displacement of well-informed advocacy necessarily becomes less justifiable." *Alderman*, 394 U.S. at 183-84.

The scope of defense review and cross-examination was left to the trial judge on remand:

> Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny which the Fourth Amendment exclusionary rule demands. It may be that the prospect of disclosure will compel the Government to dismiss some prosecutions in deference to national security authorized party interests. But this is a choice the Government concededly faces with respect to material which it has obtained illegally and which it admits, or which a judge would find, is arguably relevant to the evidence offered against the defendant.

Alderman, 394 U.S. at 184. In response to *Alderman*, Congress included 18 U.S.C. § 3504 as part of the Organized Crime Control Act of 1970. The statute requires that the government "affirm or deny" in the event an aggrieved party claims unlawful surveillance:

> **Litigation concerning sources of evidence**
>
> (a) In any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, or other authority of the United States--
>
> (1) upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act;
>
> . . . .
>
> (b) As used in this section "unlawful act" means any act the use of any electronic, mechanical, or other device (as defined in section 2510(5) of this title) in violation

> of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto.

18 U.S.C. § 3504. The legislative history establishes several things about the scope of the statute. First, by citing *Wong Sun v. United States,* 371 U.S. 471 (1963), Congress made clear that the "exploitation" language is coextensive with the fruit of the poisonous tree doctrine. 1970 U.S.C.C.A.N. at 4027 ("Section 3504(a) establishes procedures for the disposition of claims based upon allegations that evidence is the primary product of an unlawful act or has been derived from the 'exploitation' of an unlawful act."). Second, "upon a charge by the defendant with standing to challenge the alleged unlawful conduct, the Government would be required to affirm or deny that an unlawful act involving electronic surveillance had in fact occurred." *Id*.

Prior to FISA, the Supreme Court, in holding that the unlawfulness of surveillance provided a defense to contempt charges, found that § 3504 and its legislative history established the duty to affirm or deny whenever an aggrieved party claims that evidence is inadmissible because it is derived from an illegal interception. *Gelbard v. United States*, 408 U.S. 41, 58 (1972). Not many recent cases involve § 3504 beyond the grand jury stage, where it generally does not apply.[7] In the Fourth Circuit, the government argued in a grand jury case that FISA supplanted § 3504, but the court did not resolve the question. *In re Grand Jury Subpoena (T-112)*, 597 F.3d 189, 201 (4th Cir. 2010) ("The broader claims advanced as to NSA surveillance are not necessary to the disposition of this appeal, and they must await another day."). Dissenting Judge Traxler would have reached the surveillance claim and found that § 3504 applied:

---

[7] In *United States v. Hamide*, 914 F.2d 1147 (9th Cir. 1990), the government disclosed FISA surveillance in response to a discovery request in the deportation context, but the interlocutory appeal was dismissed on unrelated grounds.

> To serve its purpose, § 3504(a)(1) requires an answer that is "factual, unambiguous, [and] unequivocal," *United States v. Apple*, 915 F.2d 899, 911 (4th Cir.1990). Thus, in my view, when the government refuses to deny the illegal surveillance or provides an answer that is evasive, the aggrieved party has just cause to refuse to comply with the subpoena.

597 F.3d at 203. Based on the plain language of the statute, Judge Traxler found the notice requirement applicable to foreign intelligence surveillance. *Id*. at 203-06.

Given the repeated and explicit requests for material derived from electronic surveillance of all kinds, the government's failure to provide notice, as well as evasions regarding the existence of the surveillance, violated the plain requirements of the statute. The violation of § 3504 militates strongly in favor of full discovery and full defense participation in litigation based on the discovery.

D. The Court's Discovery Order Should Direct Full Disclosure To Security-Cleared Counsel And Full Defense Participation In Adversary Proceedings Regarding The Lawfulness Of The Government's Surveillance Activities Because The Balance Of Interests Has Tilted Sharply Toward Transparency And Inclusion Of Both Parties In All Litigation.

In the initial FISA motion, the defense described circumstances that, more than in any other reported national security case, militate in favor of defense participation: sophisticated and extensive government surveillance of an American citizen in the United States – at least in part while the citizen was a minor – who had committed no crime, whose troublesome expressions were protected by the First Amendment, and who worked for no foreign power. CR 55. The Court now has a strong indication the government's ex parte disclosures to the Court were incomplete, given that the text of the FAA notice is directed to both the Court and the defense. In the context of the disclosures over the past six months, the Court should order full participation by security-cleared defense counsel.

1. The Complexity And The Need For Accurate Factual Determinations Strongly Support Full Defense Access To Surveillance Material And Advocacy Regarding Its Significance.

The scope of appropriate disclosure to the defense corresponds to the depth and complexity of the potential motions to suppress as well as to the potential for disclosing *Brady* material. The statute provides for an aggrieved person to file a motion for suppression where the information was either unlawfully acquired or acquisition was conducted outside the scope of an order of authorization or approval. 50 U.S.C. § 1806(f). Information is unlawfully acquired if the statute is unconstitutional. *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) ("Section 1806(f) requires the court to decide whether the surveillance was 'lawfully authorized and conducted.' The Constitution is law."). The government's failure to adhere to limitations on the scope of surveillance also supports defense motions to suppress, requiring suppression of both direct and derivative evidence:

> If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person.

50 U.S.C. § 1806(g). Even if the motion is denied, the Court must review the information to determine whether material considered on the motion, assuming it was reviewed ex parte, requires production as *Brady* material: "If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." *Id.*

The statute confers authority on this Court to order disclosure to defense counsel "where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50

U.S.C. § 1806(f). In this provision, Congress intended to strike "a reasonable balance between an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself, and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information." S. Rep. No. 95-701 at 64 (1978). The developments since the Snowden disclosures and the institutionalized suppression of notice revealed after *Clapper* establish that this case – even if it is the only case – fits exactly what Congress thought should trigger full defense participation: disclosure may be "necessary" when there are "indications of possible misrepresentation of fact" and other problems indicating the need for adversarial review. *Id*.

Courts have explained that disclosure to the defense is warranted if the legal and factual issues involved in reviewing the surveillance are "complex," and where "the question of legality may be complicated by factors such as 'indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.'" *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982) (quoting S. Rep. No. 95-701 at 64 (1978)); *accord United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987). These factors must be assessed in light of *Alderman*'s recognition that valuable defense input is lost when review of the legality of electronic surveillance is conducted ex parte. 394 U.S. at 184.

2. The Balance Of The Factors This Court Considers In Determining Defense Participation Requires Full Defense Access And Advocacy.

Under the present circumstances, the balance strongly favors disclosure: the need for government secrecy has been radically reduced by the public disclosures of previously secret

programs; the need for adversary proceedings has been recognized by a presidential study group; the legal and factual complexity of the issues in this case favor full defense participation; and there are reasonable grounds to question the candor and completeness of the security apparatus's representations.

i. The Need For Secrecy Has Been Reduced By The Snowden Disclosures.

The government has either publicly acknowledged or failed to deny the broad range of electronic surveillance now attributed to the government. Prior to trial, the mass collection of telephone and Internet content and metadata was speculative; now it is fact. As a result of the Snowden disclosures and other revelations, there are no longer compelling reasons for secrecy. If the government used malware to activate Mohamed's computer to video him in his home, the existence of that capability is now public knowledge. The gathering up of all Mohamed's telephone call and Internet metadata (along with everyone else's metadata) was not previously known, but now the secret is out. The government likely has records of every one of Mohamed's calls and Internet communications prior to any FISA warrant. The only questions remaining are whether and under what circumstances the government obtained and accessed surveillance, the lawfulness of the authority or conduct of the surveillance, and how the patterns of communication can be helpful to the defense. The government need for ex parte proceedings has collapsed now that the secrets this Court was balancing against disclosure are part of general public discourse.

ii. The Benefits Of Adversarial Proceedings Are Now Recognized By The President's Review Group.

The public debate surrounding the Snowden disclosures has exposed the serious flaws that ex parte proceedings import into the structure of our country's legal system. President Obama's

national security review recognized that our adversary system is compromised, and the benefits of defense advocacy are lost, in a system that does not include an advocate for individual privacy. The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, Recommendation 28 (Dec. 12, 2013). The rationale for an advocate before the Foreign Intelligence Surveillance Court (FISC) applies equally to the need for security-cleared counsel in this case to provide technological and legal perspectives to balance against the government's one-sided presentations in proceedings before the district court:

> Our legal tradition is committed to the adversary system. When the government initiates a proceeding against a person, that person is usually entitled to representation by an advocate who is committed to protecting her interests. If it is functioning well, the adversary system is an engine of truth. It is built on the assumption that judges are in a better position to find the right answer on questions of law and fact when they hear competing views. When the FISC was created, it was assumed that it would resolve routine and individualized questions of fact, akin to those involved when the government seeks a search warrant. It was not anticipated that the FISC would address the kinds of questions that benefit from, or require, an adversary presentation. When the government applies for a warrant, it must establish "probable cause," but an adversary proceeding is not involved. As both technology and the law have evolved over time, however, the FISC is sometimes presented with novel and complex issues of law. The resolution of such issues would benefit from an adversary proceeding.

Review Group Report at 203. In our system of justice, defense counsel standing for the rights of the accused traditionally provides competing arguments needed by a neutral decision-maker.

> We have elected to employ an adversary system of criminal justice in which the parties contest all issues before a court of law. The need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts.

United States v. Nixon, 418 U.S. 683, 709 (1974). While recognizing that secrecy is sometimes permissible, this Court acts in the best traditions of our justice system by recognizing the benefits

of full adversary participation where, as here, the circumstances call for careful scrutiny of complex legal issues based on voluminous material.

iii. The Complexity Of The Legal Issues Warrants Defense Participation.

Substantial issues exist regarding the constitutionality of the FAA as well as the application of the FAA and other surveillance programs to Mohamed. These concerns were readily evident from the colloquies with several of the Justices during the *Clapper* oral argument. Justice Kagan noted that the FAA "greatly expands the government's surveillance power. Nobody denies that." Transcript of Oral Argument at 17, *Clapper*, 133 S. Ct. 1138 (2013) (No. 11-1025). Similarly, Justice Ginsburg noted that certain checks required for traditional FISA surveillance do not exist in the FAA:

> JUSTICE GINSBURG: Mr. Jaffer, could you be clear on the expanded authority under the FAA? As I understood it, it's not like in [FISA], where a target was identified and . . . the court decided whether there was probable cause. Under this new statute, the government doesn't say who the particular person or the particular location. So, there isn't that check. There isn't that check.
>
> MR. JAFFER: That's absolutely right, Justice Ginsburg…the whole point of the statute was to remove those tests, to remove the probable cause requirement, and to remove . . . the requirement that the government identify to the court the facilities to be monitored. So those are gone.
>
> That's why we use the phrase "dragnet surveillance." I know the government doesn't accept that label, but it concedes that the statute allows what it calls categorical surveillance, which . . . is essentially the surveillance the plaintiffs here are concerned about.

Id. at 32-33. Justice Breyer stated that the program is not limited to wiretapping alleged terrorists or foreign agents, noting that any conversation touching on "foreign intelligence" information could be implicated: "the definition of foreign intelligence information . . . defines it to include information

with respect to a foreign power or foreign territory that relates to the conduct of foreign affairs. It's very general." *Id*. at 43.

The competing privacy and national security interests are the subject of current judicial debate upon which the defense perspective is essential to a fair disposition. *Compare Klayman v. Obama*, No. 13-0851, 2013 WL 6571596 (D.D.C. Dec. 16, 2013) (the metadata collection program likely unconstitutional) *with ACLU v. Clapper*, No. 13 Civ. 3994, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013) (upholding the metadata collection program). The President's Review Group used collection of telephone metadata under section 215 of FISA as a "good example" of the "serious and difficult questions of statutory and constitutional interpretation about which reasonable lawyers and judges could certainly differ," finding that better decisions result from adversary presentations:

> On such a question, an adversary presentation of the competing arguments is likely to result in a better decision. Hearing only the government's side of the question leaves the judge without a researched and informed presentation of an opposing view.

Review Group Report at 203-04. The complexity of the legal questions increase with the case-factual analysis of retention, accessing, and use of information. In addition to debating the scope and lawfulness of surveillance, a defense advocate is necessary to present the legal arguments on the inclusion of false statements or material omissions within the meaning of *Franks v. Delaware*, 438 U.S. 154 (1978); on the use of evidence derived from earlier unlawful surveillance to make decisions (such as deciding not to follow the case agent's recommendation to neutralize Mohamed by arrest or cooptation) under *Murray v. United States*, 487 U.S. 533, 542-43 (1988); and determining whether the use of any such derivative evidence in subsequent FISA applications requires suppression under *United States v. Grandstaff*, 813 F.2d 1353, 1355 (9th Cir. 1987).

Further, compliance with complicated statutes upon which there is little precedent militates in favor of defense participation. The simple determination of probable cause in the standard FISA case is often "relatively straightforward and not complex." *United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010). Although the FISA issues in the present case have their own share of novelty and complexity, the complicated legal issues under the FAA receive little guidance from the courts of appeals or other districts about how to evaluate the constitutionality of orders granting applications for FAA surveillance or actual execution of the surveillance. Defense advocacy is reasonable and necessary given the serious and difficult questions this case presents.

iv. The Voluminous Factual Materials Favor Defense Participation.

The electronic surveillance generated in the national security context is far more extensive than that produced under the minimization procedures in cases investigated with Article III wiretaps. Jennifer Granick, *FISA Amendments Act Is Way Worse for Privacy Than Title III*, Center for Internet and Society of Stanford Law School, Nov. 13, 2012.[8] In contrast to Article III wiretaps, a greater volume of telephone conversations and Internet communications in national security cases are generally recorded and preserved. David S. Kris & J. Douglas Wilson, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS, 276-77 (2d ed. 2012). Minimization in national security cases generally occurs when there is a retrospective examination of bulk data and a decision is made to index and log conversations, not by contemporaneous decisions not to record conversations in compliance with Article III minimization. *Id.* National security communications that are not indexed and logged are not routinely destroyed, as with Article III material, but may still be available

[8] Available at http://cyberlaw.stanford.edu/blog/2012/11/fisa-amendments-act-way-worse-privacy-title-iii.

for defense review. *Id*. at 277. The decision of agents to treat communications as not pertinent to the foreign intelligence investigation is irrelevant to the defense assessment of whether the communication is favorable to the defense or discoverable under Rule 16 as the defendant's statement, evidence material to the defense, or otherwise subject to production. *Id*. at 278.

In this case, there is a voluminous amount of communications recorded and metadata gathered that the Court is not in a reasonable position to review. The defense is perfectly suited to review material with the full adversarial perspective, identifying potential *Brady* material, both for suppression and as trial material. In a case involving the post-trial disclosure of wiretapping, the Supreme Court noted the unique perspective of the defense in assessing the potential value of the products of government surveillance:

> An apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances. Unavoidably, this is a matter of judgment, but in our view the task is too complex, and the margin for error too great, to rely wholly on the in camera judgment of the trial court to identify those records which might have contributed to the Government's case.

Alderman, 394 U.S. at 182. The need to parse out from extensive data the information that the Court should hear is a core function of the defense that should fully apply in this case.

v. Congress Anticipated That Evidence Of Misrepresentation And Other Over-Reaching Would Favor Disclosure And Defense Participation.

The legislative history of FISA specifically stated that "indications of possible misrepresentation of fact" could establish the necessity for defense participation in discovery and suppression proceedings. S. Rep. 95-701 at 64. Congress set an intentionally low bar for favoring

defense participation: "indications" and "possible." Under this standard, which requires no finding of actual misreprentation, there are a number of factors the Court should consider as favoring defense participation.

First, the Court knows whether the government provided previous notice in chambers of which the defense is unaware due to redactions in pleadings and exclusion from chambers conferences. But it appears that, assuming the Court did not know that the derivatives of FAA surveillance were used at trial, the failure to advise the Court before trial, especially where the origins of the investigation were at issue in the non-FISA motion to suppress, constituted a serious omission. The omission of material facts, under Ninth Circuit law, constitutes the functional equivalent of a material misrepresentation for the purposes of suppression. *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir. 1985), *amended by* 769 F.2d 1410 (9th Cir. 1985). The violation of the notice statute alone should trigger full defense participation.

Second, the circumstances of the disclosure involve lack of candor high in the national security establishment. The apparent reluctance of national security lawyers to permit Solicitor General Verrilli to correct the misrepresentation to the Supreme Court reflects the kind of questionable dealings that Congress saw as favoring disclosure. Similarly, the Director of National Intelligence admitted that he provided testimony that constituted the "least untruthful" answer regarding surveillance practices before a congressional hearing. Mollie Reilly, *James Clapper: I Gave 'Least Untruthful' Answer Possible On NSA Surveillance*, Huffington Post, June 11, 2013. On March 12, 2013, Senator Ron Wyden posed the following question to NDI Clapper during a hearing of the Senate Intelligence Committee: "Does the N.S.A. collect any type of data at all on millions or hundreds of millions of Americans?" Ryan Lizza, *State of Deception*, The New Yorker,

Dec. 16, 2013. Director Clapper replied, "No, sir," explaining that no such witting activity could occur given the restrictions on CIA and NSA surveillance of Americans. After the Snowden revelations, Director Clapper submitted to the Committee a formal retraction admitting that his response was "clearly erroneous." *Id*. As Senator Wyden later stated, "There is not a shred of evidence that the statement ever would've been corrected absent the Snowden disclosures." *Id*. The erroneous testimony to Congress apparently was not an isolated incident. Kimberly Dozier, *Clapper Apologizes For "Erroneous" Answer On NSA*, Associated Press, July 2, 2013 ("Sen. Wyden is deeply troubled by a number of misleading statements senior officials have made about domestic surveillance in the past several years.").

But this type of high level deception only scratched the surface of the systematic lack of candor revealed by previously classified court decisions that the Administration released in response to the Snowden disclosures. On August 21, 2013, the government declassified the opinion of District Judge John Bates holding that aspects of the surveillance authorized by 1881a – the statute of which the government provided notice in this case – was unconstitutional. [*Case Name Redacted*], No. [docket number redacted], 2011 WL 10945618 (FISC Oct. 3, 2011). While ultimately continuing surveillance authorizations, Judge Bates made a record of serious concerns regarding the legal authority and agency actions in carrying out that authority.

The opinion detailed the government's May 2011 disclosure to the FISC that, contrary to previous statements, the NSA was relying on the FAA to collect Internet communications that are "wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection," and that the NSA "might lack confidence in the effectiveness" of procedures for ensuring that persons targeted with FAA surveillance of their

Internet transactions are actually located overseas. *Id*. at *2. In other words, the government "advised the Court that the volume and nature of the information it has been collecting is fundamentally different from what the Court had been led to believe." *Id*. at *9. These disclosures "fundamentally alter[ed] the Court's understanding of the scope of the collection conducted pursuant to Section 702," which had previously been based on erroneous representations that "acquisition of Internet communications under Section 702 would be limited to discrete 'to/from' communications between or among individual account users and to 'about' communications falling within [redacted] specific categories that had been first described to the Court in prior proceedings." *Id*. at *5.[9]

The government's applications for authorization to conduct FAA surveillance thus contained all of the problems that justify disclosure: "misrepresentation of fact, vague identification of the persons to be surveilled, [and collection of] surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards" contained in past orders. *Belfield*, 692 F.2d at 147. These problems appear to coincide temporally with the period of FAA surveillance in this case, which likely occurred between 2008 and 2010, or under earlier precursor programs.

In another opinion, Judge Bates expressed concern that, for a third time, the government acknowledged "a substantial misrepresentation" regarding surveillance:

> The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.

---

[9] Section 702 was codified as 50 U.S.C. § 1881a, the statute referenced in the government's supplemental FISA notice.

> In March, 2009, the Court concluded that its authorization of NSA's bulk acquisition of telephone call detail records from [redacted] in the so-called "big business records" matter "ha[d] been premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." Docket [redacted]. Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying. The Court concluded that this requirement had been "so frequently and systemically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively." *Id*.

[*Case Name Redacted*], No. [docket number redacted], 2011 WL 10945618, at *5 n.14 (FISC Oct. 3, 2011) (declassified on Aug. 21, 2013) (alterations in original). Other FISC judges, some in recently declassified opinions, expressed similar concerns. *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted]*, No. BR 09-13, 2009 WL 9150896, at *2 (FISC Sept. 25, 2009) (declassified Sept. 10, 2013) (the court was "deeply troubled" whether the NSA had addressed and corrected the issues giving rise to the history of serious and widespread compliance problems and had taken the necessary steps to ensure compliance going forward.); *In re Production of Tangible Things from [redacted]*, No. BR 08-13, 2009 WL 9150913, at *2 (FISC Mar. 2, 2009) (declassified Sept. 10, 2013) (detailing "misrepresentations to the Court" and "violations of its Orders"); *In re Production of Tangible Things from [redacted]*, No. BR 08-13, 2009 WL 9157881, at *2 (FISC Jan. 28, 2009) (declassified Sept. 10, 2013) ("The Court is exceptionally concerned about what appears to be a flagrant violation of its Order in this matter."); *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620–21 (FISC 2002) (explaining government's "errors related to misstatements and omissions of material

facts" in FISA applications), *abrogated on other grounds by In re Sealed Case*, 310 F.3d 717 (FISC Rev. 2002).

The errors in the government's applications to the FISC, including its applications for FAA surveillance authorization, are not merely "typographical or clerical in nature." *United States v. El-Mezain*, 664 F.3d 467, 566 (5th Cir. 2011) (internal quotation marks omitted). Rather, "the errors [are] . . . pervasive enough to confuse the court as to the quantity or quality of the evidence described in the applications," such that "disclosing the applications and related materials to defense counsel would assist the court in making an accurate determination of the legality of the surveillance." *Id.* at 567 (internal quotation marks omitted). Moreover, because numerous FISC opinions – including opinions authorizing FAA surveillance – remain classified, the defense has no way to know the full extent of the government's misrepresentations to the FISC and noncompliance with its orders. Disclosure under § 1806(f) is necessary to permit the robust adversarial testing that accurate review of these issues requires.

These misrepresentations also provide the grounds for a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). Under *Franks*, a hearing on the veracity of the affidavit supporting a warrant is required if the defendant makes a substantial showing that the affidavit contains intentional or reckless false statements or material omissions. *United States v. Jacobs*, 986 F.2d 1231, 1234-35 (8th Cir. 1993); *Stanert*, 762 F.2d at 781. *Franks* applies to applications for electronic surveillance orders as well as those seeking Rule 41 warrants. *United States v. Ippolito*, 774 F.2d 1482, 1485 (9th Cir. 1985). If the prosecution failed to disclose to the Court the then-classified FISC opinions expressing concerns regarding the reliability of the government representations, such a failure alone would be a *Franks* violation because the government omitted

material information reasonably necessary for the Court's evaluation of the government's submissions. Given the record of affirmative misrepresentations and omissions made by the government in its applications for § 1881a authorizations (as well as its misrepresentations and omissions in applications for orders authorizing other forms of FISA surveillance), full discovery is required for an adversarial hearing to assess whether the fruits of those authorizations must be suppressed.

In a separate disclosure, it has been revealed that government agents have been laundering intelligence from NSA electronic intercepts to disguise their origins: "[L]aw enforcement agents have been directed to conceal how such investigations truly begin – not only from defense lawyers but also sometimes from prosecutors and judges." John Shiffman & Kristina Cooke, *U.S. directs agents to cover up program used to investigate Americans*, Reuters, Aug. 5, 2013. The governmental units that distributed information include the FBI, the CIA, and the NSA, all of which were likely involved in the present case. Although the Reuters documents are undated, they "show that federal agents are trained to 'recreate' the investigative trail to effectively cover up where information originated." *Id*. Interviews with law enforcement personnel showed the practice is widespread to protect sources, but "employing the practice as a means of disguising how an investigation began may violate pretrial discovery rules by burying evidence that could prove useful to criminal defendants." *Id*.

The defense has expressed concerns that local prosecutors were insulated from full knowledge of surveillance and tactics used in the present case. *E.g.*, CR 42 at 10-11; CR 78 at 2-3. One of the most serious problems with *Brady* in this case apparently involved exactly this type of insulation. Long after the close of discovery, local prosecutors began discovering FBI emails, a

process that continued to the day of trial. CR 451 at 82. The emails were obvious *Brady* material, including the characterization by the FBI that Mohamed was a "conflicted/manipulable kid." CR 446 at 1466. Despite the Court's discovery orders, the prosecutor advised the Court that the tardy production occurred in part because the material was not in the case file he received. CR 451 at 88. But the existence of the emails had to have been known by the agents: the case agent and others who were on the emails themselves testified at pretrial proceedings and knew or should have known of the emails' existence and the obligation to produce them. Only at the last minute, apparently due to the prosecutor's prodding, did crucial emails, some of which became trial exhibits, surface.

The discovery order should include any material reflecting policies and practices of any agency involved in this case that insulate evidence from prosecutors and courts, including but not limited to those underlying the Reuters report.

E. The History Of Specific Defense Requests For Discovery Of All Forms Of Surveillance Provides Compelling Support For A Broad Discovery Order.

The government's failure to provide statutory notice is aggravated because the defense explicitly requested the type of electronic surveillance material that was never received. Under *Brady*, the government obligation to provide disclosure of helpful material does not depend on a defense request. *United States v. Blanco*, 392 F.3d 382, 387 (9th Cir. 2004). However, in assessing the appropriate discovery orders, the Court should consider the degree to which the government received notice from the defense that this type of material was considered helpful and the need for prosecutors to make the appropriate inquiries to all agencies actually conducting or otherwise involved in such surveillance to determine the existence of such material.

1. Defense Discovery Requests Focused On The Exact Types Of Surveillance That Are Now Known To Have Been Utilized By The Government.

Given that the existence of many of the government's electronic surveillance programs were not known at the outset of the case, the defense requested broad production of electronic surveillance. On March 7, 2011, in the initial discovery request, the defense requested material relating to "any eavesdropping, wiretapping, or electronic recording of any kind." CR 25 at 8. In the discovery memorandum, the materials were defined "as broadly as possible and without limitation." CR 27 at 10. The memorandum explicitly addressed the possibility that government evidence was "derived from" earlier investigative activity:

> The redacted discovery regarding emails after Mohamed attained the age of majority appear to indicate that the emails were "derived from" earlier investigative activity dating at least to early 2008. The degree to which the government monitored Mohamed while he was a juvenile, as well as any decisions related to whether to advise his parents, take a different course, or otherwise intervene, are important to provide context for the government's subsequent activities. Further, *any information related to monitoring would raise potential issues regarding the legal basis for such surveillance.*

CR 27 at 11 (emphasis added). Anticipating the disclosures related to mass seizure of metadata, the defense requested "all materials obtained by the government from any service provider, including Comcast, relative to Mohamed's use of the Internet should be produced." CR 27 at 16.

The discovery request broadly applied to all types of electronic surveillance that have now been disclosed both through the belated notice and the Snowden disclosures:

> The government should produce all materials connected to authorizations for monitoring, surveillance, or other investigative activity in this case. The order should encompass the application for the order, any denials of authorization, the action taken pursuant to the authorization, the products of the activity, and the uses made of the products. The order should apply to any and all uses of the FISA in addition to non-FISA activity. The FISA permits electronic surveillance (50 U.S.C. §§ 1801-11); physical searches (50 U.S.C. §§ 1821-29); pen registers and trap and

> trace devices (50 U.S.C. §§ 1841-46); and access to certain business records (50 U.S.C. §§ 1861-62). To the extent material is classified, the Court should order production under appropriate protective orders but with no limit on the access of the defense to materials that are necessary to evaluate potential suppression issues and exculpatory uses.

CR 27 at 17-18. These requests were elaborated in the FISA motion, including explicit references to potential *Franks* violations and warrantless surveillance from which the FISA warrants were derived. CR 55.

Most explicitly for the FAA notice, the defense FISA discovery request included the exact scenario that is now apparently being disclosed: the government obtained information without disclosing that it was derived from earlier warrantless activity. The defense requested that discovery regarding prior warrantless surveillance that may have generated FISA warrants: "the existence of any pre-FISA surveillance must be determined in order to litigate any FISA procedures as fruits of potential warrantless intrusions." CR 55 at 17. The defense even referenced the history of such surveillance:

> [T]here is at least some history of using warrantless surveillance as the basis for FISA requests. *See* James Bamford, THE SHADOW FACTORY, (Doubleday 2008) at 117 ("By the time the [National Security Agency] operation was up and running in the fall of 2001, between 10 and 20 percent of all the requests coming to the FISA court were tainted by what is known in the legal profession as 'the fruit of the poisonous tree,' that is, the warrantless program.").

CR 55 at 18. On *Franks*, the defense pointed to the need for discovery of potential misrepresentations and material omissions in FISA applications, which now appear to have omitted the FAA surveillance:

> The FISA applications may contain intentional or reckless material falsehoods or omissions, and the surveillance therefore may violate the principles of *Franks v. Delaware*, 438 U.S. 154 (1978). In other cases, the government has confessed error relating to "misstatements and omissions of material facts" that it had made in its

> FISA applications. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISC 2002), *abrogated on other grounds, In re Sealed Case, supra*. Disclosure is, therefore, necessary so that, based on defense analysis, this Court can conduct a *Franks* hearing at which Mohamed will have the opportunity to inquire into whether the affiants before the FISA court intentionally or recklessly made materially false statements or omitted material information from the FISA applications. In this regard, significant questions are likely to exist regarding the extent to which Mohamed was portrayed as an agent of a foreign power, whether the primary purpose of the electronic surveillance was to obtain evidence of domestic criminal activity or foreign intelligence information, whether the government made the required certifications in the FISA application, and whether it properly obtained extensions of FISA orders.

CR 55 at 17-18.

Several months later, the defense filed a supplemental memorandum advising the Court regarding concerns about use of the 2008 FISA amendments for broad surveillance activity. In this pleading the defense expressly stated:

> In the present case, the Court should consider *Clapper* as expanding the potential for facial and as applied challenges to the FAA to the extent that surveillance of Mohamed – who is unquestionably a United States person – occurred during the course of FAA-authorized operations involving non-United States persons. The discovery indicates a high likelihood that such surveillance occurred.

CR 72 at 3. Further, the defendant argued repeatedly that the trial prosecutors had an obligation to inquire broadly of all government agencies that could reasonably be believed to be in possession of relevant information. *E.g.*, CR 42 at 10; CR 58 at 44.

2. The Government's Assurances Regarding Discovery Inadequately Responded To The Discovery Requirements In This Case.

Throughout this case, the trial prosecutors told the Court that they understood their discovery obligations. *E.g.*, CR 58 at 44; CR 109 at 64; CR 159 at 70. They viewed their obligations narrowly, however, in terms of their understanding of what constituted discoverable exculpatory material and their obligation to seek out such material from other government entities. For example,

they defined their obligations under Fed. R. Crim. P. 16 as limited to material in their possession or that of "any other law enforcement agencies that are part of the prosecution team." CR 28 at 5. With respect to statements made by Mohamed, the trial prosecutors stated: "The government has complied with and will continue to comply with its obligation to produce all relevant, recorded statements of defendant." CR 28 at 18. But, the prosecutors went on to limit what they would provide stating: "as will be addressed in the government's CIPA motion, there is a national security interest in protecting much of the material from disclosure." *Id*. Later they stated:

> The government has provided, and will continue to provide, defendant with pretrial discovery in accordance with and beyond what is required by these discovery standards. Indeed, the government continues to go beyond its statutory and constitutional discovery obligations and provided the defense with a broad range of information that is not, in fact, discoverable.

CR 91 at 2. In responding to specific requests in that pleading, the government advised the Court that, with respect to the request for all materials related to the government's monitoring of statements as well as of computer activity (CR 78 at 5): "The government does not have any additional information responsive to this request." CR 91 at 7. With respect to the request for all materials relative to the search and seizure of computers, cell phones, or other electronic media, the government stated:

> The government has provided all such materials in its possession to defendant. If and when the government conducts any further analysis or searches of seized electronic material, it will be provided to defendant in accordance with the rules of discovery.

Id. at 13. In replying to the government assertions that it had provided all material in its possession, the defense provided the Court with several pleadings that described material in his possession that demonstrated that the government was in fact in possession of evidence that it had not turned over. *E.g.*, CR 99 at 5; Defendant's Third Supplement To Suppression And Discovery Motions at 4-7.

The defense requests for discovery, and government's assertions that it understood its obligations and had complied, were made not only in the pleadings, as set out above, but also in open court. Some of these statements contained troubling limitations. For example, in responding to the defense request for all of his statements, the trial prosecutor stated that he would provide all "unclassified" statements of Mohamed gathered "in conjunction" with this case. CR 58 at 18-19. These limitations appear to have been attempts to take off the table all statements gathered through undefined "other investigations" that had produced statements made by Mohamed, statements about which various agents later testified. *E.g.*, CR 446 at 1437-38. The discovery obligations of the government include no such limitations.

In responding to defense arguments about the obligation to seek out information from all government agencies, the trial prosecutor again placed a limitation on what he would do. He advised the Court that he would only make inquiries of "all associated agencies investigating the case." CR 58 at 44. When arguing a year later about provision of all website monitoring and surveillance tools on the computer, he responded that the government had no additional information. CR 109 at 20. Six months later, the trial prosecutor made similar representations in response to further defense requests for information about surreptitious investigation, stating that the government had complied with its obligations. CR 323 at 40. In addition to other apparent shortcomings in the government's statements, the provision of the new, post-trial FISA notice reveals that the government apparently had not made all the relevant inquiries or disclosures that it had repeatedly indicated to the Court that it had made. The existence of the supplemental FISA notice make clear that the government engaged in investigation and gathered evidence that it utilized in some way at trial and otherwise that was not disclosed to the defense.

3. The Record Reflects That Government Actors Failed To Adequately Communicate Discoverable Material To Local Prosecutors.

One of the points that Mohamed has been pressing throughout this litigation has been the reasonable likelihood that information was withheld from the trial prosecutors by other actors within the government. *E.g.*, CR 42 at 10-11; CR 78 at 2-3. One example of this, and the importance of an adversary process to ferret out the truth, occurred during the non-FISA suppression hearing.

In the non-FISA context, the defense established a prima facie case that, by a subterfuge, the FBI conducted an unconstitutional non-consensual search of Mohamed's laptop computer. CR 57. In arguing that the Court should not rule on the Fourth Amendment issue, the trial prosecutor offered an exhibit through the case agent to support the claim that the product of the search was not used. The agent testified that Exhibit 1 contained all of the information that Lt. Williams had obtained during his search of the computer taken from Mohamed and mirror-imaged on November 2, 2009. CR 131 at 22-24. In argument, the prosecutor made the same representation. CR 132 at 212. But both the prosecutor and the agent were wrong. Both improperly relied on assertions that had apparently been made to them by a third party. This was learned only because the defense had access to a mirror image of the hard drive, was able to examine the drive itself, and then test the government's assertions through the adversarial process. CR 159 at 16.[10]

[10] During the suppression hearing, the government made another inaccurate statement about the computer, asserting that it had only been in use for two weeks prior to its seizure on November 2. CR 131 at 23. Because this representation was able to be tested through the adversarial process, the Court learned that the computer had, in fact, been in use since September 12, 2009. CR 159 at 25. The length of time was material because it contradicted the scope of information on the computer that the government argued.

Similarly, the late production of the FBI emails should cause the Court significant concern regarding communication of discoverable materials. Although the trial prosecutors continually assured the Court that they were viewing their discovery obligations broadly, they were also making statements about limits on where they were seeking information. As was revealed with respect to the FBI emails, important evidence known to the agents was not in the case file. CR 451 at 87-88. They were, however, exculpatory, as this Court found. *Id*. at 80-81. When the government made its various ex parte CIPA filings with the Court long before December 2012, these exculpatory emails should have been produced for the Court's review. It appears that they were not. These facts underscore the danger of relying on the government's assertions when the pressures weighing against full disclosure in a national security situation are so strong.

4. Throughout The Pretrial Phase Of The Case, The Government Obscured The Extent Of Its Knowledge About Mohamed Through Investigative Activity That Occurred Prior To September 2009.

In addition to the problems with the government's response to discovery requests, the government appears to have actively impeded defense efforts to learn the truth about the origins of its investigation and the manner in which that investigation may have been derived from prior unlawful activity. In its pretrial pleadings and arguments, the government repeatedly sought to portray the origin of the investigation into Mohamed as linked solely to the call his father made to the FBI on August 31, 2009, the Khan emails, and the email Mohamed forwarded to his father that he had received from Amro al-Ali. At trial, however, the government agents were permitted to testify about the government's knowledge of Mohamed prior to September 2009 and the existence of information about him in its databases.

During the suppression hearing, when Mohamed attempted to explore the sources of the information that led to the decision to set up the undercover operation, the government repeatedly objected to questions about the origin of the investigation. For example, when asked about names on the phone taken from Mohamed on November 2, 2009, Agent Dwyer responded, "I can't answer that." CR 131 at 90. When asked whether there were further requests for authorization to search the computer taken from Mohamed on November 2, 2009, the agent again responded that he could not answer. *Id*. at 94. When asked whether the full investigation of Mohamed commenced on September 3, 2009, the agent again said that he could not answer. *Id*. at 98.

During Analyst Tanton's testimony, he was asked whether he had specific knowledge about Mohamed accessing al-Awlaki information prior to review of the computer that had been seized on November 2, 2009. CR 132 at 187-88. The government objected that this called for classified information, and its objection was sustained. *Id*. at 188. In arguing at the conclusion of the testimony on May 2, 2012, that the investigation was not tainted by the police activity on November 2, 2009, the trial prosecutor referred to three pieces of evidence that led to the investigation: the call from Mohamed's father, the Samir Khan emails, and email from Amro al-Ali. *Id*. at 216-217. He made the same argument after the reconvened hearing on June 26, 2012. CR 159 at 121. Given the discovery provided, and the truncation of testimony based on the assertion that the answers would call for classified evidence, the impression was left that all of the information on which the government was relying had been obtained on or after August 31, 2009. But those were not the facts. In contrast to the suppression hearing testimony, the trial testimony revealed some further facts about the earlier investigation. Agents Trousas and DeLong both testifed that, from government monitoring and accessing emails through another investigation, the government knew and had

information about Mohamed prior to September 2009. CR 456 at 402, 406-07; CR 446 at 1439-40, 1456-57.

The public record about the scope of government surveillance, the public record about the intelligence community's failure to be forthcoming with courts or trial prosecutors, and the public record of this case raise serious concerns about the fairness of the proceedings that led to Mohamed's conviction. These facts underscore that full adversary proceedings with participation by security-cleared counsel are needed to determine the nature and scope of surveillance and the extent to which the government's case and investigation were tainted by the previously undisclosed surveillance.

F. The Court Should Order Full Discovery Because The Origins Of This Investigation Permeated The Court's Pretrial And Trial Rulings.

The full factual background of this case should be produced to the defense because issues related to surveillance permeated the case. For example, the non-FISA motion to suppress turned upon the government's claim of independent sources for the investigation, but now we know that the government's representations regarding the reasons for governmental action were materially incomplete. Similarly, the FISA motion involved the Court's investment of trust in the completeness and candor of representations made in ex parte proceedings, and assurances that the government knew and adhered to its responsibilities, but now it appears the representations were incomplete and prevented the Court from conducting both legal analyses and discretionary decision-making regarding classified material with the full story and background facts.

At trial, the Court and the defense made decisions with inadequate and faulty information. The Court indicated its understanding of the importance to the defense of all evidence regarding the degree of government surveillance: "part of the emphasis from the defense in this case is that the

undercover individuals, the individuals who are running the undercover program, needed to put together information for a profile, that this is a way that they approach these things, they learn all they can about the individual, and that this material assisted them in putting together a profile." CR 159 at 121-22. The Court and the defense did not have information regarding the real origin and extent of the investigation; the Court and the defense did not know that, for whatever reason, the government was intentionally withholding notice that it was statutorily required to provide. Such information irremediably skewed the tactical decisions of counsel and goes to the core of the defense: not that there was no reason for governmental concern, but that the government went too far in prompting the offense.

Further, the non-disclosed indicia of governmental unreliability may have affected the discretionary decisions of the Court. For example, the Court relied on the government's ex parte representations in allowing the undercover operatives to testify under fake names and without defense investigation of their real identity. The Court also may have relied on ex parte representations in denying production of the original Arabic Interpol notice that – the defense believes – allowed the government to cast Amro al-Ali in a false light. Full discovery and defense advocacy is needed to review the potential effect of the failure to disclose on a wide range of in limine, evidentiary, and instructional rulings.

The defense will be filing substantive motions upon completion of discovery. The pervasiveness of questions regarding the origins and conduct of surveillance on Mohamed strongly militates in favor of complete full discovery to allow full development of the arguments regarding the effects of the withholding of notice regarding the extent and types of surveillance utilized in this case. Discovery that reflects on the government's reliability should be fully explored.

G. The Court Should Grant The Broadest Discovery Because Litigation Regarding The Lawfulness Of Governmental Surveillance Activity Accomplishes Important Societal Purposes Of Transparency And Deterrence.

Meaningful review regarding the government's violation of the statutory notice requirement and potential grounds for suppression of evidence accomplishes essential societal functions beyond protection of the defendant's individual rights. Constitutions and statutes are merely a collection of toothless platitudes in some countries. In the United States, transparency and deterrence of governmental misconduct are essential to the rule of law that sets us apart by giving the promise of justice meaning in the real world. Preservation of the results of a tainted three-week trial do not outweigh the strong societal interests in assuring fairness for the individual accused and assuring that the rules regarding pretrial notice and judicial review of surveillance on American citizens are protected. The public interest strongly favors full discovery and defense participation in all proceedings.

H. The Language Of The Court's Discovery Order Should Explicitly Require Broad Production And Incorporate Inclusive Language Regarding The Scope Of "Material," The Obligation To Inquire Regarding All Primary Sources, And The Use Of The Pretrial *Brady* Standard.

In the initial discovery motion, the defense requested that the Court order discovery with a number of specifications to assure complete production. The "material" sought was defined broadly: "As used herein, the term 'materials' should be construed as broadly as possible and without limitation. It includes all items in any form or medium, whether physical (*e.g.*, papers, notes, reports), or electronic *(e.g.*, e-mail, texts, or chats), analog or digital (*e.g.*, audio or video), and however created, produced, or reproduced." CR 27 at 10. The defense requested that the appropriate originating agencies be accessed to assure completeness. CR 27 at 8-9. The Court's discovery order

should include the broad definition of "material" and direction that all governmental agencies and actors be contacted and directed to produce discovery.

The Court's discovery order should require adherence to a broad interpretation of Rule 16 and the pretrial *Brady* standard. In *Hernandez-Meza*, the court indicated that, in fulfilling the discovery order on remand, it "behooves the government to interpret the disclosure requirements broadly and turn over whatever evidence it has pertaining to the case." 720 F.3d at 768-69. The same breadth is appropriate here. Further, compliance with *Brady* has been an issue throughout the case, from the failure to timely disclose that online agitator "Bill Smith" was a government agent, to the late disclosure of the FBI emails, to the failure to disclose the FAA surveillance. These problems came in the context of the government's insistence that the post-trial *Brady* standard – which requires proof of "materiality" – applied to discovery prior to trial. Over the government's objection, the Court held that materiality was not part of the standard limiting evidence favorable to the defense. But even after the Court's ruling, the government cited to the post-trial standard, relegating the Court's decision to a footnote. CR 157 at 6-7; CR 160 at 2. Given the deliberate violation of the notice statute, and the type of discovery issues precedent to the substantive motions, the Court should require that all evidence favorable to the defense or otherwise useful to the presentation of motions should be provided regardless of whether the government deems the evidence to be material. The pretrial *Brady* standard insures fairness to the defense, provides the Court with the appropriate information for decision-making, and prevents the government from benefitting from its notice violation.

Conclusion

For the foregoing reasons, the Court should order that, with full disclosure to the defense and participation in any hearings, material should be produced as follows:

- Material documenting the government's failure to provide pretrial notice of surveillance pursuant to 50 U.S.C. § 1881a, including, but not limited to, all communications manifesting any policy of non-disclosure and all communications underlying the decision to provide no notice and the decision to provide the supplemental notice. This material should at least answer the following questions:
  - * Who had knowledge that § 1881a surveillance was implicated in this case and when was such knowledge gained;
  - * Who was involved in any decision not to provide pretrial notice of § 1881a surveillance and when was such a decision made;
  - * What justification, if any, was relied upon in any decision not to provide pretrial notice of § 1881a surveillance and what led to the filing of the supplemental notice;
  - * What, if any, notice was this Court given about § 1881a surveillance relative to Mohamed (or other persons relevant to this case) prior to trial.
- Material documenting all surveillance of Mohamed and derivative use of the products of surveillance pursuant to 50 U.S.C. § 1881a. This material should at least answer the following questions:
  - * What evidence or information was gathered through surveillance about Mohamed;
  - * When was such evidence or information gathered;
  - * Under what programs and authorizations was such evidence or information gathered;
  - * What minimization and targeting procedures and interpretive instructions were in effect at the time any such evidence or information was gathered, and how were those procedures implemented (*i.e.*, who was being targeted, what was the basis for that targeting, and what minimization procedures were used during that targeting);
  - * How, when, and to or by whom was such evidence or information disseminated, accessed, or otherwise used;

* What dissemination procedures and interpretive instructions were in effect at the time any such evidence or information was gathered, accessed, and disseminated or otherwise used, and how were those procedures implemented relative to evidence or information gathered related to Mohamed;

* What justification was relied upon in conducting § 1881a surveillance, including but not limited to any FISC decisions relative to such surveillance;

* What, if anything, was this Court told about § 1881a surveillance relative to Mohamed (or other persons relevant to this case) in deciding pretrial discovery and suppression motions and trial evidentiary rulings;

* What, if anything, was the FISC told about § 1881a surveillance relative to Mohamed (or other persons relevant to this case) in approving any FISA warrants in this case.

- Material documenting all surveillance of Mohamed (other than pursuant to § 1881a) and derivative use of the products of surveillance that has not been disclosed to the defense. This material should at least answer the following questions:

  * What evidence or information was gathered pursuant to other sections of FISA, including but not limited to §§ 1842, 1861, 1881b, and 1881c;

  * What evidence or information was gathered pursuant to other surveillance or information gathering programs implemented by any government agency that has not been disclosed to the defense, including but not limited to the use of malware or spyware to access and exploit Mohamed's computer, and any other surveillance activities conducted by any government agency;

  * How was any such evidence or information identified, collected, and retained;

  * How, when, and to or by whom, was any such evidence or information disseminated, accessed, or otherwise used;

  * What was the legal justification, if any, related to the collection and use of such evidence or information;

  * What were any minimization, targeting, retention, and dissemination procedures and interpretive instructions in place relative to any surveillance described above and how were those procedures implemented relative to Mohamed;

  * What, if anything, was this Court told about such evidence or information (and the means by which it was obtained) in deciding pretrial discovery and suppression motions and trial evidentiary rulings;

* What, if anything, was the FISC told about such evidence or information (and the means by which it was obtained) in approving any FISA warrants in this case.

- Material favorable to the defense under the pretrial *Brady* standard, statements of the defendant, and evidence material to the preparation of the defense, both as to motions and trial. This material should at least answer the following questions:

  * What classified judicial opinions included findings that government surveillance policies and practices were conducted beyond the scope of authorizations or were otherwise unlawful;

  * What evidence demonstrates government over-reaching during national security investigations, such as unlawful searches, intrusions into privacy, false statements, material omissions, and violations of statutory or other rules;

  * What evidence shows programs or practices that discouraged or barred disclosure to prosecutors and courts of information that is discoverable under rules, statutes, or the Constitution, including but not limited to government policies and training to cover up the source of NSA-obtained information.

The government's violation of the statutory notice requirement and the pervasive overall surveillance issues raise serious legal issues on which full factual development is warranted. This discovery motion seeks to identify for the Court the areas on which discovery is required so legal briefing can proceed on a complete factual record. For all of the foregoing reasons, the discovery motion should be granted.

Dated this 13th day of January, 2014.

/s/ Stephen R. Sady
Stephen R. Sady
Chief Deputy Federal Public Defender

/s/ Steven T. Wax
Steven T. Wax
Federal Public Defender

/s/ Lisa Hay
Lisa Hay
Assistant Federal Public Defender